(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 363 122 B1**

(12) # EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: **21.12.94 Bulletin 94/51**

(51) Int. Cl.[5]: **G07F 7/10**

(21) Application number: **89310051.1**

(22) Date of filing: **02.10.89**

(54) **Transaction authentication system.**

(30) Priority: **03.10.88 JP 249561/88**

(43) Date of publication of application: **11.04.90 Bulletin 90/15**

(45) Publication of the grant of the patent: **21.12.94 Bulletin 94/51**

(84) Designated Contracting States: **DE FR GB**

(56) References cited:
EP-A- 0 086 286
EP-A- 0 198 384
EP-A- 0 220 703
EP-A- 0 234 954
EP-A- 0 281 058
WO-A-85/03787
US-A- 4 529 870

(73) Proprietor: **FUJITSU LIMITED**
1015, Kamikodanaka
Nakahara-ku
Kawasaki-shi Kanagawa 211 (JP)

(72) Inventor: **Ogasawara, Nobuo**
3-35-21-201, Nukuikitamachi
Koganei-shi Tokyo, 184 (JP)
Inventor: **Ozaki, Yoshiyuki**
3-34-9, Nokendai
Kanazawa-ku
Yokohama-shi Kanagawa, 236 (JP)

(74) Representative: **Stebbing, Timothy Charles et al**
Haseltine Lake & Co.
Hazlitt House
28 Southampton Buildings
Chancery Lane
London WC2A 1AT (GB)

EP 0 363 122 B1

Description

BACKGROUND OF THE INVENTION

The present invention generally relates to transaction authentication systems, and more particularly to a transaction authentication system which authenticates a transaction which uses an integrated circuit (IC) card after the transaction is made.

Presently, transactions using cards are popular due to their convenience. But on the other hand, illegal use of such cards is increasing and it is becoming more and more important to authenticate the transactions.

Conventionally, when authenticating a transaction which uses a magnetic stripe card, a verified data is generated within a terminal device in conformance with a predetermined algorithm and is added to a transaction data. The uniqueness of the data is used when discriminating whether or not the transaction is correctly performed.

For example, the magnetic stripe card is loaded on a point-of-sales (POS) terminal or the like when using a credit service. Prior to making a transaction, a check is made to prevent illegal use of the magnetic stripe card. For example, a personal identification number (PIN) is entered by the user and the POS terminal discriminates whether or not the entered PIN corresponds with a PIN which is prerecorded on the magnetic stripe card, and the POS terminal discriminates whether or not the use of the magnetic stripe card on the POS terminal is permitted based on a terminal confirmation code. After it is discriminated that the PIN entered by the user corresponds with the PIN prerecorded on the magnetic stripe card and that the use of the magnetic stripe card is permitted on the POS terminal, the POS terminal adds verified data to the transaction data and temporarily stores the data on a recording medium. The verified data is generated within the POS terminal in conformance with a predetermined algorithm. For example, the recording medium is a flexible disc. After the transaction ends, a transaction historical information is transferred to a host computer within an operation center or the like by a batch data transmission.

The character of the verified data differs from that of the PIN in that the user is unaware of the existence of the verified data and the verified data is not used for prohibiting the transaction. Normally, a check is made after the transaction is made to determine whether or not the value of the verified data is in conformance with the generating algorithm so as to discriminate whether or not the transaction made was legitimate.

However, a person who is familiar with the operations and functions of the POS terminal may easily decode a program for generating the verified data. Furthermore, a person who somehow finds out the generating algorithm for generating the verified data may easily and freely operate the POS terminal without using a magnetic stripe card. Such persons can make an illegal transaction by fabricating or altering the transaction data and the verified data. When making the illegal transaction, such persons can easily make the verified data which is added to the illegal transaction data take a value in conformance with the generating algorithm, and in this case, it is impossible to find out that an illegal transaction was made. An integrated circuit (IC) card also suffers a similar problem because the verified data is generated and added to the transaction data within the terminal.

US-A-4 529 870 discloses a transaction authentication system whose object is to prevent an illegal transaction from being made. A card includes encrypted account data, including an account balance, which is updated at each transaction performed by inserting the card in a terminal. This account data also includes "check numbers", which are combined with (e.g. decrypted using) a secret owner ID supplied by the user, so as to prevent unauthorised use of the card. The check numbers may be wholly predetermined and pre-stored on the card in advance. After receiving transaction data including a check number assigned to the transaction, the terminal can forward the data to a central clearing house for debiting the account. However, there is no use of historical transaction data for authenticating transactions which have already taken place. The system relies on encryption of data on the card and of communication between the data and terminal, in order to prevent unauthorised access to the data on the card or eavesdropping of transmitted data. Thus, illegal transactions are prevented from being made in the first place.

EP-A-0 234 954 discloses a self-contained card that does not require interaction with a terminal in order to enter a PIN. The user enters a PIN directly into the card itself; the card then produces a transaction identification code (TIC) which varies for each transactional use of the card. The TIC can then be verified by passing the card through a card reader or the like.

According to the present invention, there is provided a transaction authentication system comprising terminal means comprising first processing means and a card reader/writer; first memory means; and an integrated circuit card which is detachably loaded into said card reader/writer, said card comprising second processing means and second memory means, wherein said terminal means supplies transaction data which is related to a transaction and a designated storage region in said second memory means for storing the transaction data in said card when said card accesses a service via said terminal means; said second processing means of said card writes the transaction data received from said terminal means in the designated storage region of said second memory

means, and also generates verified data which is renewed every time the transaction data is written into said second memory, said verified data having a value in conformance with a predetermined generating algorithm, said verified data being stored in said second memory means and also supplied to said terminal means; and said first processing means of said terminal means generates transaction historical information which includes at least the designated storage region, the transaction data and the verified data and stores the transaction historical information in said first memory means, whereby a transaction is authenticatable by comparing the verified data stored in said first memory means (12, 18) and the verified data stored in said second memory means, non-correspondence of the verified data indicating that an illegal transaction has been made.

Thus, verified data which is unique for each transaction is stored within the IC card and is also supplied to the terminal means to be stored in the first memory means. Hence, it is possible to authenticate the transaction by verifying the verified data stored within the IC card and the first memory means. The verified data cannot be fabricated or altered even by a person who is familiar with the programs of the terminal means, and the reliability of the IC card is greatly improved compared to the conventional case because illegal transactions can easily be found.

Reference is made, by way of example, to the accompanying drawings, in which:-

Fig. 1 is a system block diagram for explaining an operating principle of a transaction authentication system according to the present invention;

Fig. 2 is a system block diagram of a first embodiment of the Fig. 1 system;

Fig. 3 is a system block diagram showing an embodiment of an IC card used in the first embodiment;

Figs. 4A and 4B respectively are a perspective view and a system block diagram for explaining the embodiment of the IC card shown in Fig. 3 in more detail;

Fig. 5 is a system block diagram of an IC card used in a second embodiment;

Figs. 6A, 6B and 6C respectively are flow charts for explaining an operation of a central processing unit of the IC card shown in Fig. 5; and

Fig. 7 is a side view in cross-section generally showing an embodiment of a card reader/writer which is used in the second embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

First, a description will be given of an operating principle of a transaction authentication system according to the present invention, by referring to FIG.1. The transaction authentication system generally comprises an IC card 1, a terminal 9, and a memory device 12. The IC card 1 comprises a processor 2, a first memory 3 which prestores a plurality of processing means (or programs) for operating the processor 2, and a second memory 4 which stores a transaction data which is processed by the operation of the processor 2. When making a transaction using the IC card 1, the transaction authentication system starts the transaction after authenticating a specific information which is stored in the IC card 1. The second memory 4 includes transaction data storage regions 8 which are respectively designated for each transaction and storage regions 27 which respectively store a transaction execution identifying information for each transaction in correspondence with a transaction data storage region 8. The processor 2 includes a write means 5 for designating the transaction data storage region 8 and for storing a transaction data therein, a verified data generating means 6 for generating a verified data for a transaction based on the transaction execution identifying information, and a renewing means 7 for renewing the transaction execution identifying information within the storage region 27 every time the transaction data is received.

The IC card 1 is loaded into the terminal 9 which can read and write information with respect to the IC card 1. The terminal 9 comprises a transaction processing means 10 for executing a transaction after the specific information of the IC card 1 is confirmed, and a transaction historical information generating means 11 for generating a transaction historical information in which a transaction data is added with a verified data which is read from the IC card 1 and an information which designates the transaction data storage region 8 for each transaction. The memory device 12 stores the transaction historical information which is received from the terminal 9.

The transaction is made as follows. That is, when the IC card 1 is loaded into the terminal 9, the terminal 9 reads a card identification information (for example, a card name) from the IC card 1 via a route which is not shown in FIG.1 and starts the transaction if the PIN can be confirmed. A transaction data which is obtained by the start of the transaction is output from the transaction processing means 10. The transaction data and an address data which designates a write address within the IC card 1 are supplied to the transaction historical information generating means 11 within the terminal 9 and the write means 5 and the renewing means 7 within the IC card 1.

The write means 5 writes the received transaction data at a designated address of the transaction data storage region 8 of the second memory 4. The renewing means 7 reads the transaction execution identifying information from an address of the storage region 27 set depending on the designated address, and renews the value of the transaction execution identifying information for every transaction.

The renewed transaction execution identifying information is written into the storage region 27 and the renewing means 7 supplies to the verified data generating means 6 an information which designates the region into which the renewed transaction execution identifying information is written.

The verified data generating means 6 uses the information which is received from the renewing means 7 to read out the renewed transaction execution identifying information from the storage region 27 and to generate the verified data. This verified data is supplied to the transaction historical information generating means 11 within the terminal 9.

The transaction historical information generating means 11 receives the verified data, the transaction data from the transaction processing means 10 and the information for designating the region within the IC card 1. The transaction historical information generating means 11 generates a transaction historical information which includes at least these three kinds of data and supplies the transaction historical information to the memory device 12.

Accordingly, when the transaction historical information is generated within the terminal 9 without the use of the IC card 1, the value of the verified data of the IC card 1 is no longer in conformance with the generating algorithm. Even when the transaction is made, the value of the verified data included in the transaction historical information which is stored in the memory device 12 after the transaction is different from the value of the verified data which is generated from the transaction execution identifying information which is renewed for every transaction and is stored in the second memory 4 of the IC card 1.

Next, a description will be given of a first embodiment of the transaction authentication system according to the present invention, by referring to FIG.2. In FIG.2, those parts which are basically the same as those corresponding parts in FIG.1 are designated by the same reference numerals, and a description thereof will be omitted. In FIG.2, a POS terminal 20 corresponds to the terminal 9 shown in FIG.1, and an IC card 21 corresponds to the IC card 1 shown in FIG.1.

FIG.3 shows an embodiment of the IC card 21. In FIG.3, those parts which are basically the same as those corresponding parts in FIG.1 are designated by the same reference numerals, and a description thereof will be omitted. The processor 2 of the IC card 21 comprises the first memory 3, the second memory 4, the write means 5, an adder means 24, a serial number generating means 25 and a serial number informing means 26. The adder means 24, the serial number generating means 25 and the serial number informing means 26 correspond to the verified data generating means 6 and the renewing means 7.

When the IC card 21 receives a write command from the POS terminal 20 and the transaction data which is included within the parameter of the write command as the write data, the write means 5 of the processor 2 stores the transaction data into the transaction data storage region 8 of the second memory 4. On the other hand, when storing the transaction data, the adder means 24 adds a constant value to an initial value and the added value (serial number) is stored in the storage region 27 of the second memory as the transaction execution identifying information. The added value is thereafter supplied to the serial number generating means 25.

The serial number generating means 25 generates a serial number as the verified data. In this case, the serial number generating means 25 outputs the transaction execution identifying information (added value which is a serial number) as it is. The transaction execution identifying information (serial number) becomes "0" when forming the transaction data storage region 8 and is thereafter incremented by one, for example, every time the transaction data is written. Hence, the transaction execution identifying information is for example a serial number x_1, x_2, ...

The serial number is returned to the POS terminal 20 via the serial number informing means 26.

The hardware structure of the IC card 21 itself is known. FIGS.4A and 4B respectively are a perspective view and a system block diagram for explaining the IC card 21 shown in FIG.3 in more detail. The IC card 21 shown in FIGS.4A and 4B comprises a central processing unit (CPU) 30 which corresponds to the processor 2, a read only memory (ROM) 31 which corresponds to the first memory 3, an electrically erasable programmable ROM (EEPROM) 32 which corresponds to the second memory 4, and contacts 33 for signal input/output.

The CPU 30, the ROM 31 and the EEPROM 32 which are made up of semiconductor elements have extremely small sizes and is capable of making complex signal processings and providing large memory capacities. For this reason, unlike the magnetic stripe card which is limited to a single function, the IC card 21 can be used to receive a plurality of services with the same card. For example, the services may include a credit service, deposits and savings services, a hospital service, various private club services and the like. In addition, even when the IC card 21 is used to receive only the credit service, for example, the same card may be used for transactions with a plurality of stores and offices, accounts provided independently for each of the stores and offices, accounts in a plurality of banks and the like.

The IC card 21 is loaded into a card reader/writer (not shown) which is connected to the POS terminal 20. The card reader/writer reads from the IC card 21 the card identification information which identifies the IC card 21, and supplies the card identification information to a host computer (not shown). The host computer returns to the POS terminal a region desig-

nating information and the like for 20 designating a transaction data storage region 8 within the IC card 21.

Prior to making the transaction using the IC card 21, a check is made to prevent illegal use of the IC card 21. For example, a personal identification number (PIN) is entered by the user and the POS terminal 20 discriminates whether or not the entered PIN corresponds with a PIN which is prerecorded on the IC card 21, and the POS terminal 20 discriminates whether or not the use of the IC card 21 on the POS terminal 20 is permitted based on a terminal confirmation code.

Next, a description will be given of an operation of the first embodiment by referring to FIG.2. When the user uses the IC card 21 and purchases an item having a price of 200 dollars, for example, the operator of the POS terminal 20 loads the IC card 21 into the card reader/writer of the POS terminal 20 and enters the transaction sum of 200 dollars into the POS terminal 20. In this case, the transaction processing means 10 of the POS terminal 20 outputs a transaction sum data of 200 dollars and a transaction date data which includes the year, month and date of the transaction. The transaction processing means 10 further designates the storage region (area) where the transaction sum data and the transaction date data are to be stored. Based on the data received from the transaction processing means 10, the write means 5 of the IC card 21 writes the transaction data (transaction sum data and transaction date data) in a designated area A of the second memory 4. Then, the serial number generating means 25 of the IC card 21 generates the serial number. This serial number is stored in an internal memory and is supplied to the POS terminal 20.

The transaction historical information generating means 11 of the POS terminal 20 adds the serial number which is received from the IC card 21 to the transaction data (transaction sum data and transaction date data), the card identification information (for example, a card ID "CARD001") of the IC card 21, and the region designating information (area A in this case), so as to generate a unique transaction historical information among the plurality of IC cards, a plurality of POS terminals and a plurality of transaction data. The transaction historical information is written into the memory device 12 via a storing means 14. After the transaction ends, the transaction historical information is written into a memory device 18 within a host terminal 22 via communication means 15 and 16 and a storing means 17 by a batch data transmission.

The transaction is completed in the above described manner. When the transaction is legitimate, the serial numbers within the transaction historical information stored in the memory devices 12 and 18 change regularly in conformance with the generating algorithm. Hence, it is possible to authenticate the transaction by checking the change in the values of the serial numbers. When the transaction is legitimate, the serial number stored in the IC card 21 constantly corresponds with the serial number of the last transaction stored in the memory devices 12 and 18.

For example, the transaction historical information received from the POS terminal 20 may have been generated by an illegal user who not only knows the PIN but also knows the generating algorithm for the serial number. Such an illegal user can operate the POS terminal 20 and generate the transaction historical information without actually using the IC card 21. In this case, it is impossible to prohibit the illegal transaction itself, however, the serial numbers stored in the memory devices 12 and 18 after the transaction is made become different from the serial number stored in the IC card 21. Therefore, it is possible to find out that the illegal transaction has been made by verifying the serial number stored in the IC card 21 and the serial numbers stored in the memory devices 12 and 18, since the stored serial numbers do not correspond in the case of the illegal transaction.

In the first embodiment, the serial number is used as the verified data. However, it is possible to use a function as the verified data. In this case, the transaction execution identifying information x is taken as an argument and the verified data generating means 6 generates a function F(x). For example, the transaction execution identifying information x has an initial value x_0 and is renewed for every transaction such that the transaction execution identifying information x has a value x_k when a kth transaction is made.

The function generated by the verified data generating means 6 need not necessarily be a single argument function and may be a multiple argument function. In the case of the multiple argument function, n arguments (x_1, x_2, x_3, ..., x_n) are renewed for every transaction.

The transaction execution identifying information for example has the initial value x_0 and values x_1, x_2, x_3, ..., x_k which are calculated for every transaction. All of these values of the transaction execution identifying information may be stored in the storage region 27 of the second memory 4. As an alternative, it is also possible to store only the final value x_k of the transaction execution identifying information in the storage region 27 of the second memory 4.

Next, a description will be given of a second embodiment of the transaction authentication system according to the present invention. FIG.5 shows an embodiment of the IC card used in the second embodiment of the transaction authentication system according to the present invention. In FIG.5, an IC card 51 comprises a terminal group 52, an input/output interface 53, a CPU 54, drivers 55, 56 and 57, a random access memory (RAM) 58, a ROM 59, an EEPROM 60, and a system bus 61.

The terminal group 52 comprises a power source

terminal Vcc for receiving a power source voltage, a ground terminal GND for receiving a ground voltage, a reset terminal RST for receiving a reset signal, a programming terminal Vpp for receiving a programming voltage, a clock terminal CLK for receiving a clock signal, and an input/output terminal I/O for inputting and outputting serial data. The terminals of the terminal group 52 other than the input/output terminal I/O are connected to the CPU 54. The input/output terminal is connected to the input/output interface 53.

The input/output interface 53 converts a serial input data into a parallel input data. When a predetermined number of bits of data (for example, four to eight bits of data) is received, the input/output interface 53 interrupts the CPU 54 by sending an interrupt signal. On the other hand, when sending a data from the IC card 51 to a terminal (not shown), the data is output serially from the input/output interface 53 via the input/output terminal I/O of the terminal group 52. When outputting the data from the IC card 51, the CPU 54 sets a parallel data (for example, eight bits) in the input/output interface 53 and the set data is automatically output via the input/output terminal I/O with a timing determined by the clock signal received from the clock terminal CLK.

The drivers 55, 56 and 57 respectively drive the RAM 58, the ROM 59 and the EEPROM 60. The input/output interface 53, the CPU 54, the drivers 55 through 57, the RAM 58, the ROM 59 and the EEPROM 60 are coupled by the system bus 61. The system bus 61 is made up of an address bus 61a, a data bus 61b, and an input/output control bus 61c. For example, the address bus 61a and the data bus 61b respectively are 8-bit buses. The input/output control bus 61c is used for transmitting the clock signal, the ground voltage, the power source voltage, the interrupt signal and the like.

The RAM 58 is used as a work area for the CPU 54 when making calculations and the like during the transaction. The ROM 59 stores programs of the CPU 54 and corresponds to the ROM 31 shown in FIGS.4A and 48. The EEPROM 60 stores the account number, PIN, balance of the account, transaction history, final transaction information, transaction historical information and the like and corresponds to the EEPROM 32 shown in FIGS.4A and 4B.

The IC card 51 is used on a terminal such as the POS terminal 20 described before in conjunction with the first embodiment.

FIGS.6A, 6B and 6C respectively are flow charts for explaining an operation of the CPU 54 of the IC card 51 shown in FIG.5. In FIG.6A, when an internal process of the IC card 51 is started and a card ID request is received, a step S1 reads the card ID from the EEPROM 60. The read card ID is supplied to the terminal and a desired service is selected from the terminal. A step S2 reads a service name of the selected service from the ROM 59. A step S3 discriminates whether or not the service name is found in the ROM 59. When the discrimination result in the step S3 is NO, a selection error information is supplied to the terminal. But when the discrimination result in the step S3 is YES, a step S4 requests authentication to the terminal. The terminal then supplies an authenticate code or key (PIN) which is necessary to make the selection, and a step S5 develops the authenticate code which corresponds to the selected service from the EEPROM 60 to the RAM 58. A step S6 develops an error number counter in the RAM 58.

A step S7 discriminates whether or not the authenticate code which is received from the terminal corresponds with the authenticate code which is developed in the RAM 58. When the discrimination result in the step S7 is YES, a step S8 clears the error number counter and stores the authenticate code in the EEPROM 60. A step S9 stores in the EEPROM 60 an information which indicates that the authentication is ended, and the authentication end information is supplied to the terminal and the process advances to a step S21 shown in FIG.6B.

On the other hand, when the discrimination result in the step S7 is NO, a step S10 increments the counted value in the error number counter and stores the incremented value in the EEPROM 60. A step S11 discriminates whether or not the counted value in the error number counter is greater than a predetermined number. When the discrimination result in the step S11 is NO, a legitimacy error information is supplied to the terminal. But when the discrimination result in the step S11 is YES, a step S12 sets a lock flag within the EEPROM 60 to an ON state and a locked state information is supplied to the terminal. When the lock flag is ON, the IC card 51 is made unusable for the selected service, and a locked state information is supplied to the terminal. In other words, the lock flag indicates whether or not the selected service is accessible by the IC card 51.

As described before, the IC card 51 may be used to receive various services. Hence, it is inconvenient if the IC card 51 were made unusable for all the services even when only predetermined one or more services should actually be made non-accessible. Therefore, in actual practice, the error number counter is provided for each service and the predetermined number used for the comparison in the step S11 is set for each service. In other words, a lock flag is provided for each service accessible by the IC card 51. For the sake of convenience, a description will hereunder be given of a case where only one lock flag is provided.

In FIG.6B, a transaction information write command including a transaction information and a write position within the IC card 51 is received from the terminal. A step S21 reads an authentication completion information, and a step S22 reads the lock flag. A step

S23 discriminates whether or not the lock flag is ON. When the discrimination result in the step S23 is YES, a locked state information is supplied to the terminal. On the other hand, when the discrimination result in the step S23 is NO, a step S24 discriminates whether or not the authentication is ended. When the discrimination result in the step S24 is NO, an authentication error information is supplied to the terminal. When the discrimination result in the step S24 is YES, a step S25 develops the access qualification information of the user in accordance with the authentication information from the EEPROM 60 to the RAM 58.

A step S26 discriminates whether or not the user has a right to write information. When the discrimination result in the step S26 is NO, an access qualification error information is supplied to the terminal. But when the discrimination result in the step S26 is YES, a step S27 transfers the necessary information from the EEPROM 60 to the RAM 58 and a step S28 discriminates whether or not a designated write position exists. When the discrimination result in the step S28 is NO, a designation error information is supplied to the terminal. On the other hand, when the discrimination result in the step S28 is YES, a step S29 writes the data at the designated write position within the RAM 58. A step S30 develops the transaction serial number from the EEPROM 60 to the RAM 58, and a step S31 increments the transaction serial number in the RAM 58. The process then advances to a step S41 shown in FIG.6C.

In FIG.6C, the step S41 by calculation generates the verified data in conformance with a generating algorithm based on unique numbers such as the transaction serial number and the transaction date. A step S42 stores the verified data in the RAM 58. A step S43 discriminates whether or not all of the processes are correctly ended. When the discrimination result in the step S43 is NO, a write error information is supplied to the terminal. On the other hand, when the discrimination result in the step S43 is YES, a step S44 stores the write information, the verified data and the transaction serial number in the EEPROM 60. A step S45 discriminates whether or not the data are correctly stored in the EEPROM 60 in the step S44. When the discrimination result in the step S45 is NO, a memory error information is supplied to the terminal. When the discrimination result in the step S45 is YES, a step S46 assembles the transmitting data and an end information including a normal end information and the verified data is supplied to the terminal. When a transaction end information is received from the terminal, a step S47 ends the process by releasing the RAM 58 and the process is ended.

FIG.7 generally shows an embodiment of a card reader/writer which is used in the second embodiment. Of course a similar card reader/writer may be used in the first embodiment. In FIG.7, a card reader/writer 70 generally comprises a card inserting opening 71, a magnetic head 72, a timing belt 73, a card transport path 74, a contact part 75, a motor 76, a roller 77, a printed circuit 78 which has the CPU 54, the ROM 59 and the like arranged thereon, and a cover 79 which is indicated by a phantom line.

When the IC card 51 is inserted into the card inserting opening 71, the IC card 51 is transported along the card transport path 74 by a transport mechanism to a loaded position where contacts of the contact part 75 make contact with the corresponding terminals of the terminal group 52 of the IC card 51. The transport mechanism includes the motor 76 which rotates the roller 77 so as to drive the timing belt 73.

In this embodiment, the magnetic head 72 is provided to read a magnetic stripe of the IC card 51. The provision of the magnetic head 72 enables the card reader/writer 70 to read the magnetic stripes of both the IC card 51 and the conventional magnetic. In other words, there is card interchangeability among the IC cards and the magnetic stripe cards. However, it is not essential to provide the magnetic head 72 on the card reader/writer 70. In addition, the card reader/writer 70 may be a part of the terminal or be a unit independent of the terminal.

Further, the present invention is not limited to these embodiments, but various variations and modifications may be made without departing from the scope of the present invention as defined in the claims.

Claims

1. A transaction authentication system comprising terminal means (9, 20) comprising first processing means (10, 11) and a card reader/writer (70); first memory means (12, 18); and an integrated circuit card (1, 21, 51) which is detachably loaded into said card reader/writer, said card comprising second processing means (2, 30, 54) and second memory means (3, 4, 31, 32, 58, 59, 60); wherein said terminal means (9, 20) supplies transaction data which is related to a transaction and a designated storage region in said second memory means (3, 4, 31, 32, 58, 59, 60) for storing the transaction data in said card (1, 21, 51) when said card accesses a service via said terminal means; said second processing means (2, 30, 54) of said card writes the transaction data received from said terminal means in the designated storage region of said second memory means, and also generates verified data which is renewed every time the transaction data is written into said second memory, said verified data having a value in conformance with a predetermined generating algorithm, said verified data being stored in said second memory means and also supplied to said terminal means; and said first processing means

(10, 11) of said terminal means generates transaction historical information which includes at least the designated storage region, the transaction data and the verified data and stores the transaction historical information in said first memory means, whereby a transaction is authenticatable by comparing the verified data stored in said first memory means (12, 18) and the verified data stored in said second memory means, non-correspondence of the verified data indicating that an illegal transaction has been made.

2. The transaction authentication system as claimed in claim 1, characterized in that said first memory means (12) is connected to said terminal means (9, 20) and is provided exclusively for said terminal means.

3. The transaction authentication system as claimed in claim 1, characterized in that said first memory means (18) is coupled to said terminal means (9, 20) via communication means (15, 16).

4. The transaction authentication system as claimed in any of claims 1 to 3, characterized in that said terminal means (9, 20) is constituted by a point-of-sales terminal (20).

5. The transaction authentication system as claimed in any of claims 1 to 4, characterized in that said integrated circuit card (1, 21, 51) further comprises a terminal group (33, 52) which is coupled to said second processing means (30, 54), said card reader/writer (70) of said terminal means (9, 20) reading/writing serial data with respect to said integrated circuit card via said terminal group.

6. The transaction authentication system as claimed in any of claims 1 to 5, characterized in that said second processing means (30, 54) of said integrated circuit card (1, 21, 51) generates a serial number as the verified data.

7. The transaction authentication system as claimed in any of claims 1 to 5, characterized in that said second processing means (30, 54) of said integrated circuit card (1, 21, 51) generates an n-argument function as the verified data, where n = 1, 2, ...

8. The transaction authentication system as claimed in any of claims 1 to 5, characterized in that said second processing means (30, 54) of said integrated circuit card (1, 21, 51) generates as the verified data a value which is unique for each transaction.

9. The transaction authentication system as claimed in any of claims 1 to 8, characterized in that said second processing means (30, 54) of said integrated circuit card (1, 21, 51) stores in said second memory means (3, 4, 31, 32, 58, 59, 60) only a verified data which is generated with respect to a last transaction.

10. The transaction authentication system as claimed in any of claims 1 to 9, characterized in that said second memory means (3, 4, 31, 32, 58, 59, 60) comprises a first memory (31, 59) for storing programs for carrying out processes on said second processing means (30, 54) and a second memory (32, 60) for storing data.

11. The transaction authentication system as claimed in claim 10, characterized in that said first memory (31, 59) is constituted by a read only memory and said second memory (32, 60) is constituted by an electrically erasable programmable read only memory.

12. The transaction authentication system as claimed in claim 10, characterized in that said second memory means (3, 4, 31, 32, 58, 59, 60) further comprises a third memory (58) for providing a work area for said second processing means (30, 54).

13. The transaction authentication system as claimed in claim 12, characterized in that said third memory (58) is constituted by a random access memory.

14. The transaction authentication system as claimed in any of claims 1 to 13, characterized in that said second processing means (30, 54) includes means for setting a lock flag when an authenticate code which is received from said terminal means (9, 20) and corresponds to a selected service differs from an authenticate code stored in said second memory means (3, 4, 31, 32, 58, 59, 60) a predetermined number of times, said first lock flag which is set indicating that the selected service is non-accessible.

15. The transaction authentication system as claimed in claim 14, characterized in that said lock flag is set independently for each service.

16. The transaction authentication system as claimed in any of claims 1 to 15, characterized in that said second processing means (30, 54) comprises write means (5) for writing the transaction data which is received from said terminal means (9, 20) into the designated storage region of said second memory means (3, 4, 31, 32, 58, 59, 60),

renewing means (7) for renewing a transaction execution identifying information which is stored in said second memory means every time the transaction data is received from said terminal means, and verified data generating means (6) for generating the verified data based on the transaction execution identifying information read from said second memory means.

17. The transaction authentication system as claimed in claim 16, characterized in that said verified data generating means (6) supplies the transaction execution identifying information which is read from said second memory means (3, 4, 31, 32, 58, 59, 60) as it is to said terminal means (9, 20) as the verified data.

18. The transaction authentication system as claimed in any of claims 1 to 17, characterized in that said second memory means (3, 4, 31, 32, 58, 59, 60) stores a card identification information, said second processing means (30, 54) of said integrated circuit card (1, 21, 51) supplies the card identification which is read from said second memory means together with the verified data, and said first processing means (10, 11) of said terminal means (9, 20) generates the transaction historical information which also includes the card identification information.

Patentansprüche

1. Ein Transaktionsauthentisierungssystem mit einem Terminalmittel (9, 20), das erste Verarbeitungsmittel (10, 11) und einen Kartenleser/-schreiber (70) umfaßt; ersten Speichermitteln (12, 18); und einer Karte mit integrierter Schaltung (1, 21, 51), die in den genannten Kartenleser/schreiber herausnehmbar geladen wird, welche Karte ein zweites Verarbeitungsmittel (2, 30, 54) und zweite Speichermittel (3, 4, 31, 32, 58, 59, 60) umfaßt; bei dem das genannte Terminalmittel (9, 20) Transaktionsdaten liefert, die sich auf eine Transaktion und eine bezeichnete Speicherzone in den genannten zweiten Speichermitteln (3, 4, 31, 32, 58, 59, 60) zum Speichern der Transaktionsdaten in der genannten Karte (1, 21, 51) beziehen, wenn die genannte Karte über das genannte Terminalmittel auf einen Dienst zugreift; das genannte zweite Verarbeitungsmittel (2, 30, 54) der genannten Karte die Transaktionsdaten, die von dem genannten Terminalmittel empfangen wurden, in die bezeichnete Speicherzone der genannten zweiten Speichermittel schreibt und auch verifizierte Daten erzeugt, die jedes Mal, wenn die Transaktionsdaten in den genannten zweiten Speicher geschrieben werden, erneuert werden, welche verifizierten Daten einen Wert gemäß einem vorbestimmten Erzeugungsalgorithmus haben, welche verifizierten Daten in den genannten zweiten Speichermitteln gespeichert werden und auch dem genannten Terminalmittel zugeführt werden; und die genannten ersten Verarbeitungsmittel (10, 11) des genannten Terminalmittels Transaktionsverlaufsinformationen erzeugen, die wenigstens die bezeichnete Speicherzone, die Transaktionsdaten und die verifizierten Daten enthalten, und die Transaktionsverlaufsinformationen in den genannten ersten Speichermitteln speichern, wodurch eine Transaktion authentisierbar ist, indem die verifizierten Daten, die in den genannten ersten Speichermitteln (12, 18) gespeichert sind, und die verifizierten Daten, die in den genannten zweiten Speichermitteln gespeichert sind, verglichen werden, wobei ein Nichtübereinstimmen der verifizierten Daten anzeigt, daß eine illegale Transaktion vorgenommen worden ist.

2. Das Transaktionsauthentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß das genannte erste Speichermittel (12) mit dem genannten Terminalmittel (9, 20) verbunden ist und ausschließlich für das genannte Terminalmittel vorgesehen ist.

3. Das Transaktionsauthentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß das genannte erste Speichermittel (18) mit dem genannten Speichermittel (9, 20) über Kommunikationsmittel (15, 16) gekoppelt ist.

4. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß das genannte Terminalmittel (9, 20) durch ein Kassenterminal (20) gebildet ist.

5. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die genannte Karte mit integrierter Schaltung (1, 21, 51) ferner eine Anschlußgruppe (33, 52) umfaßt, die mit dem genannten zweiten Verarbeitungsmittel (30, 54) gekoppelt ist, bei dem der genannte Kartenleser/-schreiber (70) des genannten Terminalmittels (9, 20) serielle Daten bezüglich der genannten Karte mit integrierter Schaltung über die genannte Anschlußgruppe liest/schreibt.

6. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß das genannte zweite Verarbeitungsmittel (30, 54) der genannten Karte mit integrierter Schaltung (1, 21, 51) als verifizierte Daten eine laufende Nummer erzeugt.

7. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß das genannte zweite Verarbeitungsmittel (30, 54) der genannten Karte mit integrierter Schaltung (1, 21, 51) als verifizierte Daten eine n-Argumentenfunktion erzeugt, wobei n = 1, 2, ... ist.

8. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß das genannte zweite Verarbeitungsmittel (30, 54) der genannten Karte mit integrierter Schaltung (1, 21, 51) als verifizierte Daten einen Wert erzeugt, der für jede Transaktion eindeutig ist.

9. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß das genannte zweite Verarbeitungsmittel (30, 54) der genannten Karte mit integrierter Schaltung (1, 21, 51) in den genannten zweiten Speichermitteln (3, 4, 31, 32, 58, 59, 60) nur verifizierte Daten speichert, die bezüglich einer letzten Transaktion erzeugt wurden.

10. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß die genannten zweiten Speichermittel (3, 4, 31, 32, 58, 59, 60) einen ersten Speicher (31, 59) zum Speichern von Programmen zum Ausführen von Verfahren bei dem genannten zweiten Verarbeitungsmittel (30, 54) und einen zweiten Speicher (32, 60) zum Speichern von Daten umfassen.

11. Das Transaktionsauthentisierungssystem nach Anspruch 10, dadurch gekennzeichnet, daß der genannte erste Speicher (31, 59) durch einen Nur-Lese-Speicher gebildet ist und der genannte zweite Speicher (32, 60) durch einen elektrisch löschbaren programmierbaren Nur-Lese-Speicher gebildet ist.

12. Das Transaktionsauthentisierungssystem nach Anspruch 10, dadurch gekennzeichnet, daß die genannten zweiten Speichermittel (3, 4, 31, 32, 58, 59, 60) ferner einen dritten Speicher (58) zum Vorsehen eines Arbeitsbereichs für das genannte zweite Verarbeitungsmittel (30, 54) umfassen.

13. Das Transaktionsauthentisierungssystem nach Anspruch 12, dadurch gekennzeichnet, daß der genannte dritte Speicher (58) durch einen Speicher mit wahlfreiem Zugriff gebildet ist.

14. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 13, dadurch gekennzeichnet, daß das genannte zweite Verarbeitungsmittel (30, 54) ein Mittel enthält, zum Setzen eines Verriegelungsflags, wenn sich ein Authentisierungskode, der von dem genannten Terminalmittel (9, 20) empfangen wird und einem ausgewählten Dienst entspricht, von einem Authentisierungskode, der in den genannten zweiten Speichermitteln (3, 4, 31, 32, 58, 59, 60) gespeichert ist, vorbestimmte Male unterscheidet, welches erste Verriegelungsflag, das gesetzt ist, anzeigt, daß der ausgewählte Dienst nicht zugänglich ist.

15. Das Transaktionsauthentisierungssystem nach Anspruch 14, dadurch gekennzeichnet, daß das genannte Verriegelungsflag für jeden Dienst unabhängig gesetzt wird.

16. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 15, dadurch gekennzeichnet, daß das genannte zweite Verarbeitungsmittel (30, 54) ein Schreibmittel (5) umfaßt, zum Schreiben von Transaktionsdaten, die von dem genannten Terminalmittel (9, 20) empfangen wurden, in die bezeichnete Speicherzone der genannten zweiten Speichermittel (3, 4, 31, 32, 58, 59, 60), ein Erneuerungsmittel (7) zum Erneuern von Transaktionsausführungskenninformationen, die in den genannten zweiten Speichermitteln gespeichert sind, jedes Mal, wenn die Transaktionsdaten von dem genannten Terminalmittel empfangen werden, und ein Erzeugungsmittel von verifizierten Daten (6) zum Erzeugen der verifizierten Daten auf der Grundlage von Transaktions- ausführungskenninformationen, die aus den genannten zweiten Speichermitteln gelesen wurden.

17. Das Transaktionsauthentisierungssystem nach Anspruch 16, dadurch gekennzeichnet, daß das genannte Erzeugungsmittel von verifizierten Daten (6) die Transaktionsausführungskenninformationen, die aus den genannten zweiten Speichermitteln (3, 4, 31, 32, 58, 59, 60) gelesen wurden, dem genannten Terminalmittel (9, 20) als verifizierte Daten zuführt wie sie sind.

18. Das Transaktionsauthentisierungssystem nach irgendeinem der Ansprüche 1 bis 17, dadurch gekennzeichnet, daß die genannten zweiten Speichermittel (3, 4, 31, 32, 58, 59, 60) Kartenkenninformationen speichern, das genannte zweite Verarbeitungsmittel (30, 54) der genannten Karte mit integrierter Schaltung (1, 21, 51) das Kartenkennzeichen, das aus den genannten zweiten Speichermitteln gelesen wurde, zusammen mit den verifizierten Daten liefert, und die genannten ersten Verarbeitungsmittel (10, 11) des genannten Terminalmittels (9, 20) die Transaktionsver-

laufsinformationen erzeugen, die auch die Kartenkenninformationen enthalten.

Revendications

1. Système d'authentification de transaction, comprenant des moyens formant terminal (9, 20) comprenant des premiers moyens de traitement (10, 11) et un lecteur/enregistreur de cartes (70), des premiers moyens formant mémoire (12, 18); et une carte à circuit intégré (1, 21, 51) qui est introduite de façon détachable dans ledit lecteur/enregistreur de cartes, ladite carte comprenant des deuxièmes moyens de traitement (2, 30, 54) et des deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60); dans lequel lesdits moyens formant terminal (9, 20) fournissent des données de transaction qui sont relatives à une transaction et à une zone de mémorisation désignée dans lesdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60) pour mémoriser les données de la transaction sur ladite carte (1, 21, 51) lorsque ladite carte accède à un service par l'intermédiaire desdits moyens formant terminal; lesdits deuxièmes moyens de traitement (2, 30, 54) de ladite carte écrivent les données de la transaction reçues desdits moyens formant terminal dans la zone de mémorisation désignée desdits deuxièmes moyens formant mémoire et produisent des données vérifiées qui sont renouvelées chaque fois que les données de la transaction sont écrites dans ladite deuxième mémoire, lesdites données vérifiées ayant une valeur conforme à un algorithme générateur prédéterminé, lesdites données vérifiées étant mémorisées dans lesdits deuxièmes moyens formant mémoire et en outre fournies auxdits moyens formant terminal; et lesdits premiers moyens de traitement (10, 11) desdits moyens formant terminal produisent des informations d'historique de la transaction qui comprennent au moins la zone de mémorisation sésignée, les données la transaction et les données vérifiées, et mémorisent les informations d'historique de la transaction dans lesdits premiers moyens formant mémoire, ce par quoi une transaction est authentifiable en comparant les données vérifiées mémorisées dans lesdits premiers moyens formant mémoire (12, 18) et les données vérifiées mémorisées dans lesdits deuxièmes moyens formant mémoire, la non-correspondance des données vérifiées indiquant qu'une transaction illégale a été effectuée.

2. Système d'authentification de transaction selon la revendication 1, caractérisé en ce que lesdits premiers moyens formant mémoire (12) sont reliés auxdits moyens formant terminal (9, 20) et sont prévus exclusivement pour lesdits moyens formant terminal.

3. Système d'authentification de transaction selon la revendication 1, caractérisé en ce que lesdits premiers moyens formant mémoire (18) sont reliés auxdits moyens formant terminal (9, 20) par des moyens de télécommunications (15, 16).

4. Système d'authentification de transaction selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdits moyens formant terminal (9, 20) sont constitués par un terminal de point de vente (20).

5. Système d'authentification de transaction selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite carte à circuit intégré (1, 21, 51) comprend en outre un groupe de bornes (33, 52) qui est relié auxdits deuxièmes moyens de traitement (30, 54), ledit lecteur/enregistreur de cartes (70) desdits moyens formant terminal (9, 20) lisant ou écrivant des données série sur ladite carte à circuit intégré par l'intermédiaire dudit groupe de bornes.

6. Système d'authentification de transaction selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdits deuxièmes moyens de traitement (30, 54) de ladite carte à circuit intégré (1, 21, 51) produisent un numéro de série comme données vérifiées.

7. Système d'authentification de transaction selon l'une quelconque des revendications 1 à 5, caractérisé en ce que lesdits deuxièmes moyens de traitement (30, 54) de ladite carte à circuit intégré (1, 21, 51) produisent une fonction à n arguments comme données vérifiées, où n = 1, 2, ...

8. Système d'authentification de transaction selon l'une des revendications 1 à 5, caractérisé en ce que lesdits deuxièmes moyens de traitement (30, 54) de ladite carte à circuit intégré (1, 21, 51) produisent comme données vérifiées une valeur qui est unique pour chaque transaction.

9. Système d'authentification de transaction selon l'une des revendications précédentes, caractérisé en ce que lesdits deuxièmes moyens de traitement (30, 54) de ladite carte à circuit intégré (1, 21, 51) mémorisent dans lesdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60) uniquement des données vérifiées qui sont produites pour la dernière transaction.

10. Système d'authentification de transaction selon

l'une des revendications 1 à 9, caractérisé en ce que lesdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60) comprennent une première mémoire (31, 59) pour mémoriser des programmes pour exécuter des traitements dans lesdits deuxièmes moyens de traitement (30, 54) et une deuxième mémoire (32, 60) pour mémoriser des données.

11. Système d'authentification de transaction selon la revendication 10, caractérisé en ce que ladite première mémoire (31, 59) est constituée par une mémoire morte et ladite deuxième mémoire (32, 60) est constituée par une mémoire morte programmable effaçable électriquement.

12. Système d'authentification selon la revendication 10, caractérisé en ce que lesdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60) comprennent en outre une troisième mémoire (58) pour fournir une zone de travail pour lesdits deuxièmes moyens de traitement (30, 54).

13. Système d'authentification de transaction selon la revendication 12, caractérisé en ce que ladite troisième mémoire (58) est constituée par une mémoire vive.

14. Système d'authentification de transaction selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdits deuxièmes moyens de traitement (30, 54) comprennent des moyens pour établir un drapeau de verrouillage quand un code authentique qui est reçu desdits moyens formant terminal (9, 20) et correspond à un service sélectionné diffère d'un code d'authentification mémorisé dans lesdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60) un nombre prédéterminé de fois, ledit drapeau de verrouillage qui est établi indiquant que le service sélectionné n'est pas accessible.

15. Système d'authentification de transaction selon la revendication 14, caractérisé en ce que ledit drapeau de verrouillage est établi indépendamment pour chaque service.

16. Système d'authentification de transaction selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdits deuxièmes moyens de traitement (30, 54) comprennent des moyens d'écriture (5) pour écrire les données de la transaction qui sont reçues desdits moyens formant terminal (9, 20) dans la zone de mémorisation désignée desdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60), des moyens de renouvellement (7) pour renouveler une information identifiant l'exécution d'une transaction qui est mémorisée dans lesdits deuxième moyens formant mémoire chaque fois que les données de la transaction sont reçues desdits moyens formant terminal, et des moyens générateurs de données vérifiées (6) pour produire les données vérifiées sur la base de l'information identifiant l'exécution de la transaction lue dans lesdits deuxième moyens formant mémoire.

17. Système d'authentification de transaction selon la revendication 16, caractérisé en ce que lesdits moyens générateurs de données vérifiées (6) fournissent l'information identifiant l'exécution de la transaction qui est lue dans lesdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60) telle qu'elle est auxdits moyens formant terminal (9, 20) comme données vérifiées.

18. Système d'authentification de transaction selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdits deuxièmes moyens formant mémoire (3, 4, 31, 32, 58, 59, 60) mémorisent une information d'identification de carte, lesdits deuxièmes moyens de traitement (30, 54) de ladite carte à circuit intégré (1, 21, 51) fournit l'identification de la carte qui est lue dans lesdits deuxièmes moyens formant mémoire avec les données vérifiées, et lesdits premiers moyens de traitement (10, 11) desdits moyens formant terminal (9, 20) produisent les informations d'historique de la transaction qui comprennent également l'information d'identification de la carte.

FIG. 1

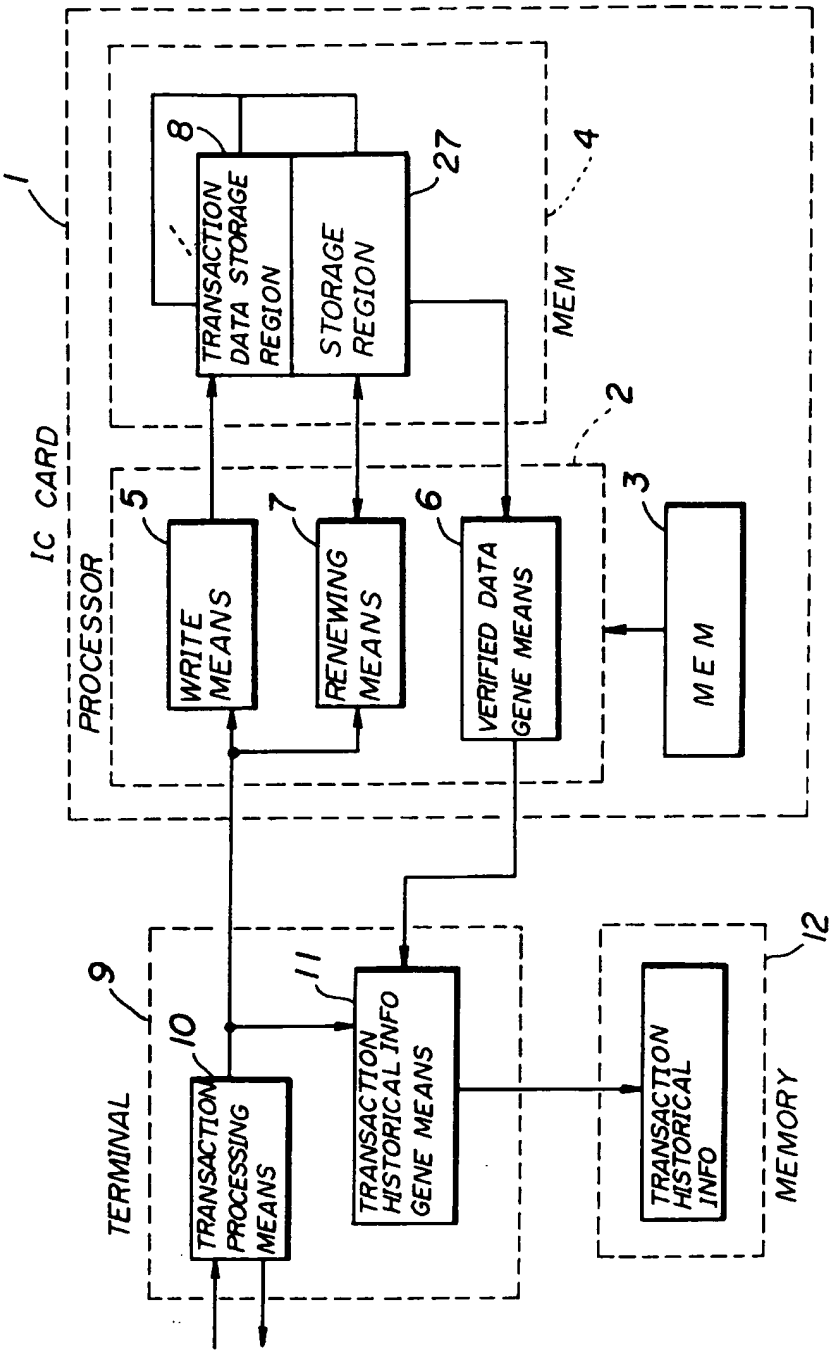
1
IC CARD
PROCESSOR
2
MEM
4
8
TRANSACTION DATA STORAGE REGION
27
STORAGE REGION
5
WRITE MEANS
7
RENEWING MEANS
6
VERIFIED DATA GENE MEANS
3
MEM
9
TERMINAL
10
TRANSACTION PROCESSING MEANS
11
TRANSACTION HISTORICAL INFO GENE MEANS
12
TRANSACTION HISTORICAL INFO
MEMORY

FIG.2

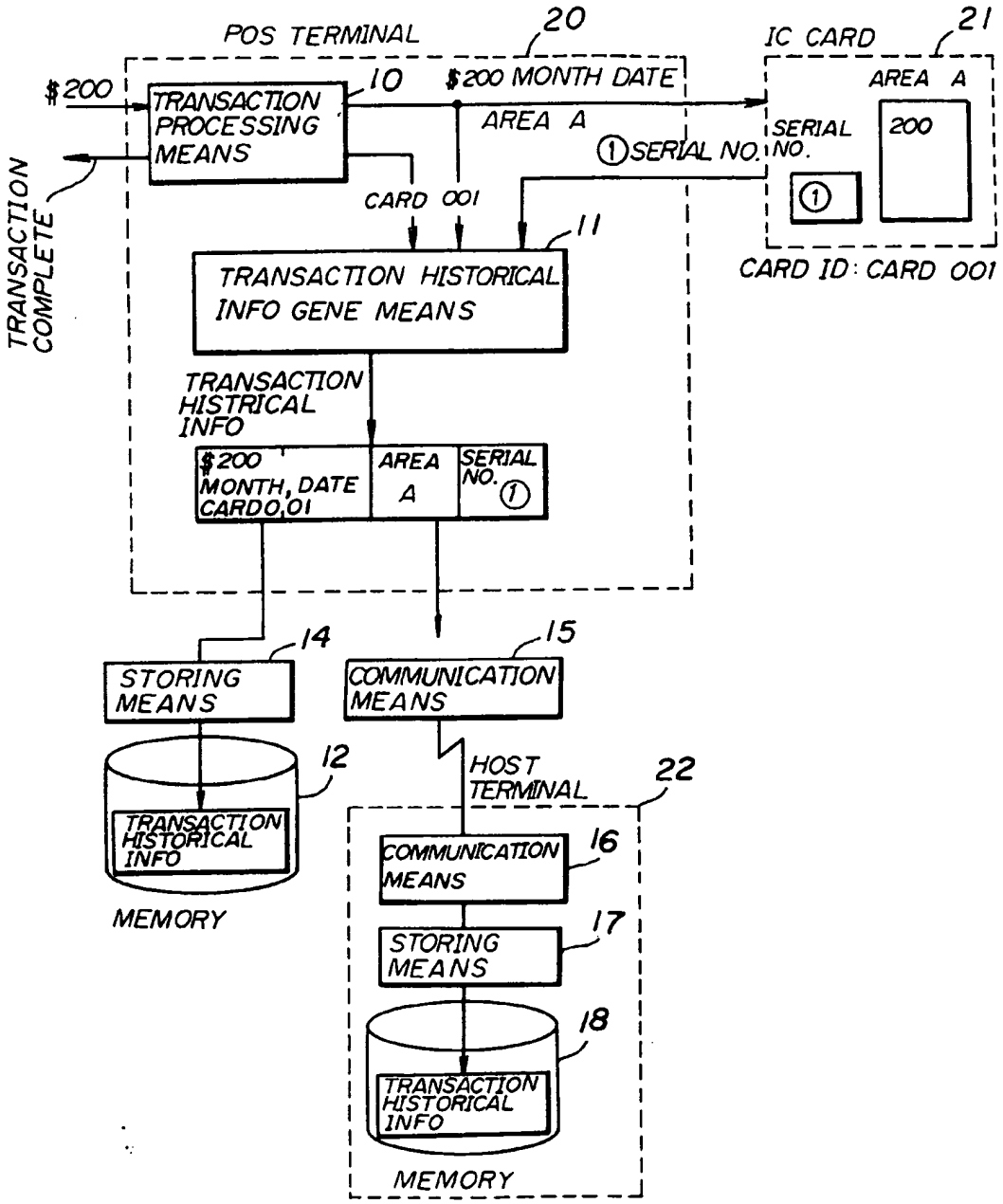
POS TERMINAL
20
IC CARD
21
$200
TRANSACTION PROCESSING MEANS
10
$200 MONTH DATE
AREA A
①SERIAL NO.
AREA A
SERIAL NO.
200
①
TRANSACTION COMPLETE
CARD 001
11
TRANSACTION HISTORICAL INFO GENE MEANS
CARD ID: CARD 001
TRANSACTION HISTRICAL INFO
$200 MONTH, DATE CARD0,01
AREA A
SERIAL NO. ①
14
15
STORING MEANS
COMMUNICATION MEANS
12
HOST TERMINAL
22
TRANSACTION HISTORICAL INFO
MEMORY
16
COMMUNICATION MEANS
17
STORING MEANS
18
TRANSACTION HISTORICAL INFO
MEMORY

FIG.3

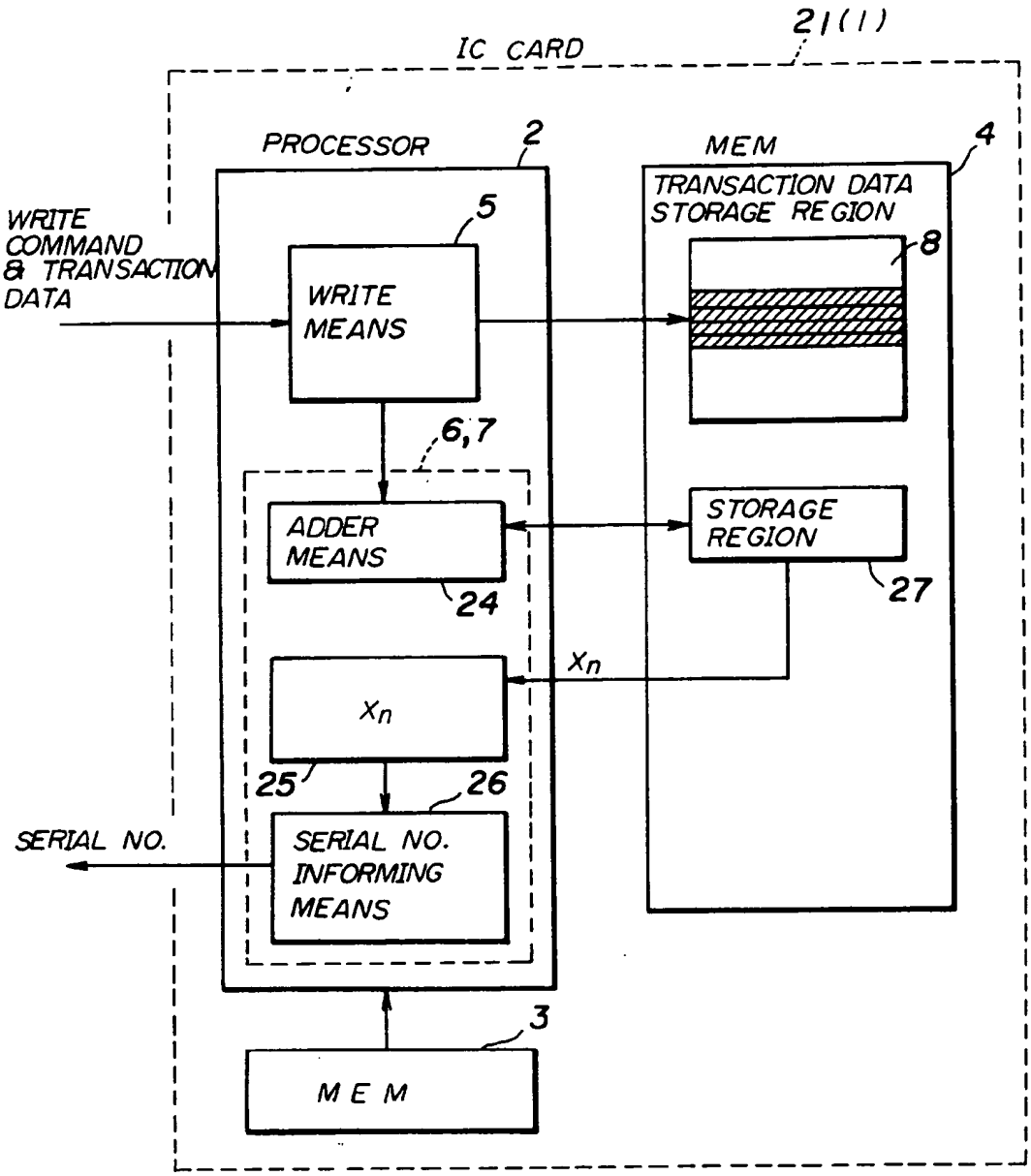
21(1)
IC CARD
PROCESSOR
2
MEM
4
TRANSACTION DATA STORAGE REGION
8
WRITE COMMAND & TRANSACTION DATA
5
WRITE MEANS
6,7
ADDER MEANS
24
STORAGE REGION
27
Xn
Xn
25
26
SERIAL NO.
SERIAL NO. INFORMING MEANS
3
M E M

FIG. 4A

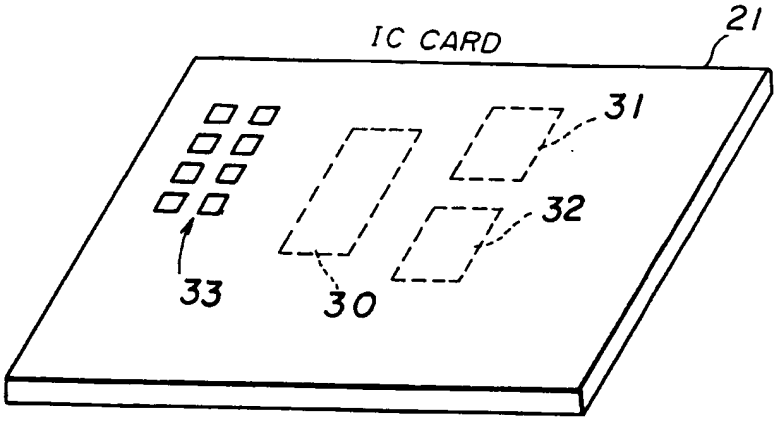
IC CARD
21
31
32
33
30

FIG. 4B

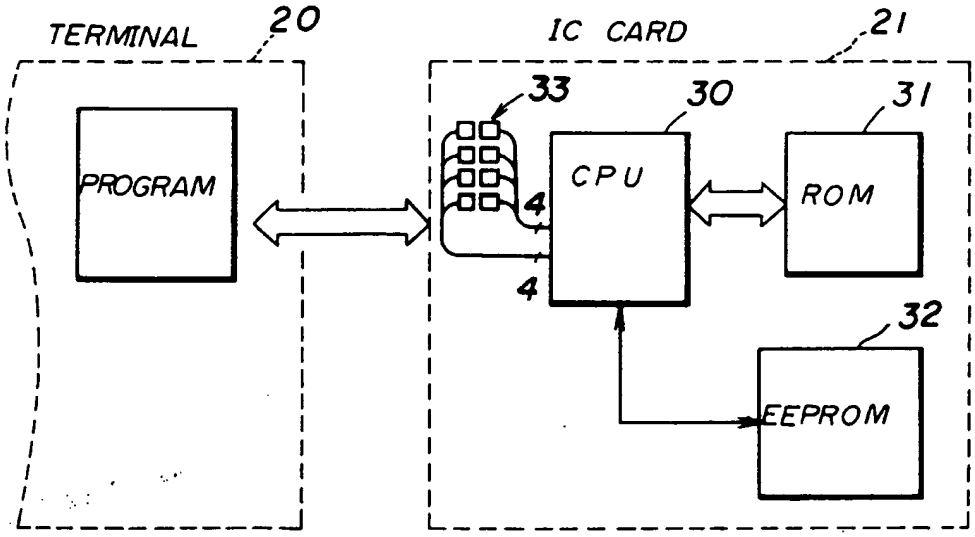
TERMINAL
20
PROGRAM
IC CARD
21
33
30
31
CPU
ROM
4
4
32
EEPROM

FIG. 5

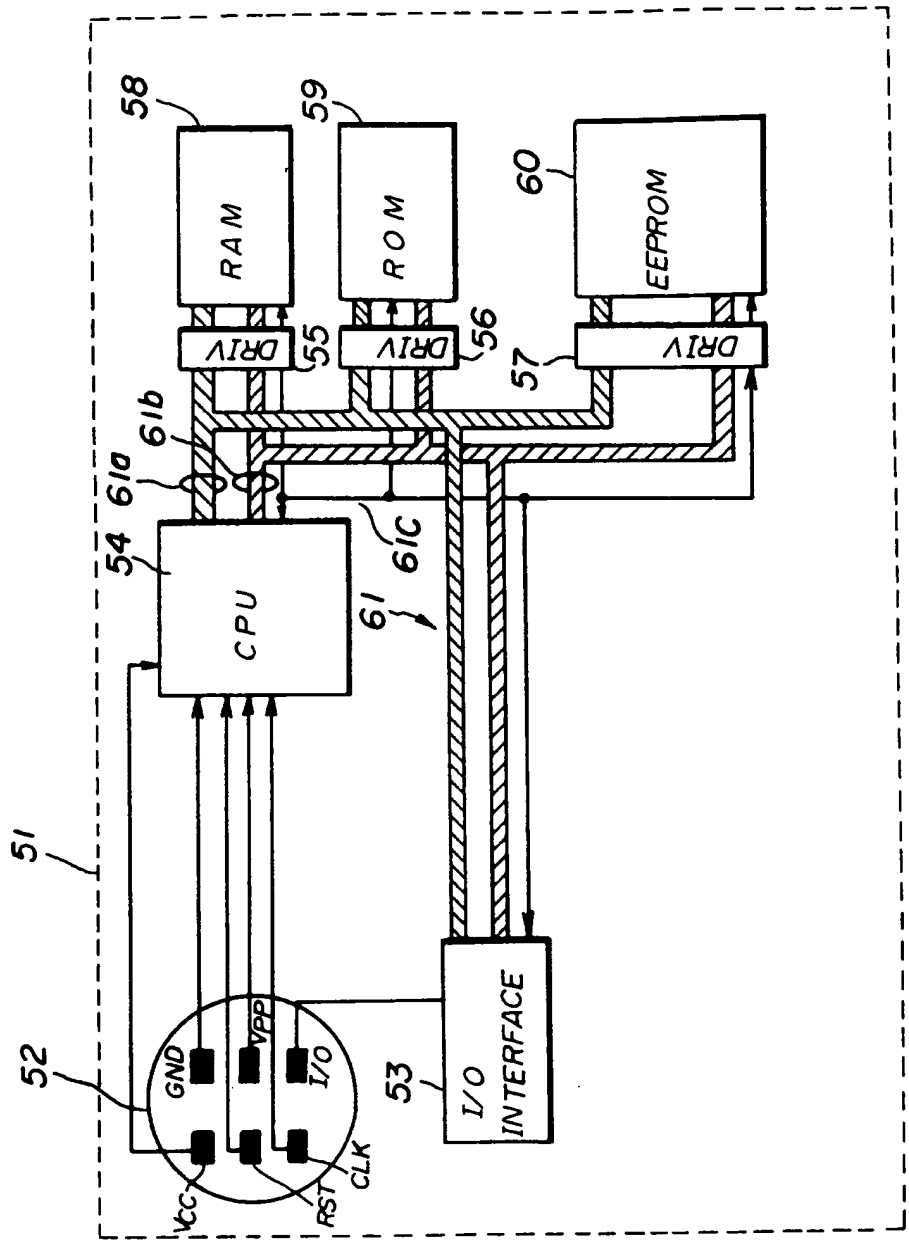
58
59
60
RAM
ROM
EEPROM
DRIV
55
56
57
61b
61a
61c
54
CPU
61
51
52
GND
VPP
I/O
CLK
RST
VCC
53
I/O
INTERFACE

FIG.6A

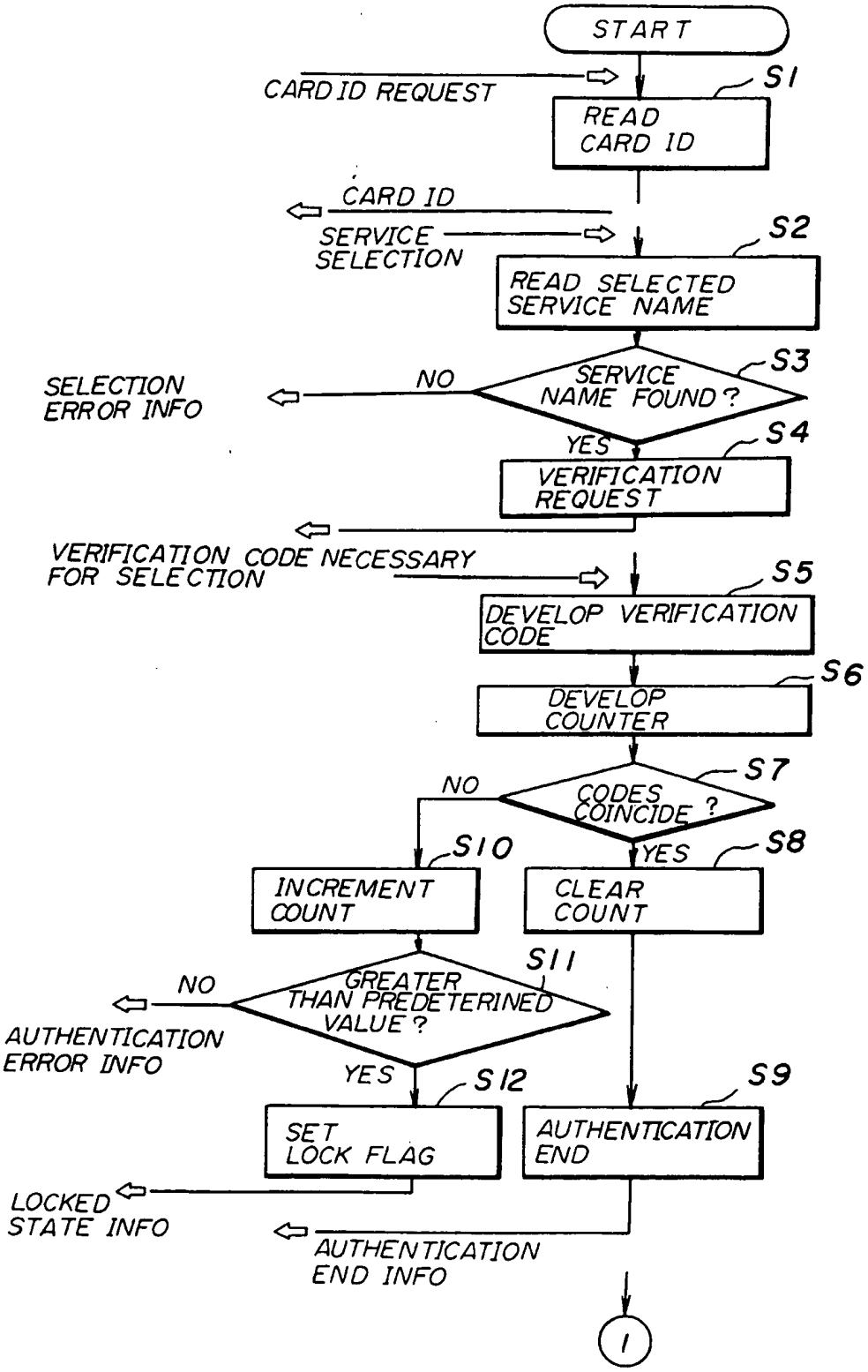
START
CARD ID REQUEST
S1
READ CARD ID
CARD ID
SERVICE SELECTION
S2
READ SELECTED SERVICE NAME
S3
SERVICE NAME FOUND ?
NO
SELECTION ERROR INFO
YES
S4
VERIFICATION REQUEST
VERIFICATION CODE NECESSARY FOR SELECTION
S5
DEVELOP VERIFICATION CODE
S6
DEVELOP COUNTER
S7
CODES COINCIDE ?
NO
YES
S10
INCREMENT COUNT
S8
CLEAR COUNT
S11
GREATER THAN PREDETERINED VALUE ?
NO
AUTHENTICATION ERROR INFO
YES
S12
SET LOCK FLAG
S9
AUTHENTICATION END
LOCKED STATE INFO
AUTHENTICATION END INFO
1

FIG.6B

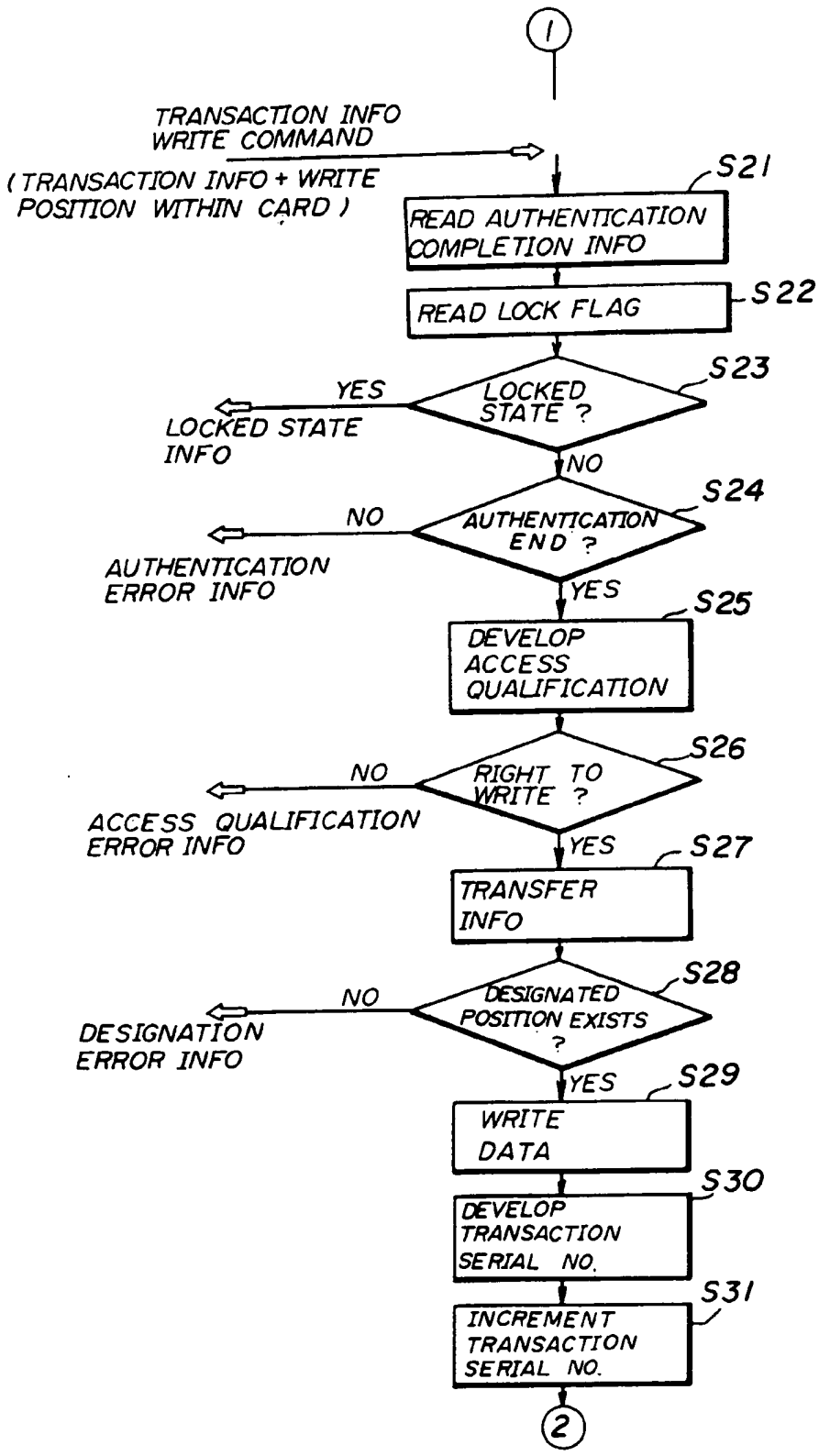
1
TRANSACTION INFO WRITE COMMAND
(TRANSACTION INFO + WRITE POSITION WITHIN CARD)
S21
READ AUTHENTICATION COMPLETION INFO
S22
READ LOCK FLAG
S23
LOCKED STATE ?
YES
LOCKED STATE INFO
NO
S24
AUTHENTICATION END ?
NO
AUTHENTICATION ERROR INFO
YES
S25
DEVELOP ACCESS QUALIFICATION
S26
RIGHT TO WRITE ?
NO
ACCESS QUALIFICATION ERROR INFO
YES
S27
TRANSFER INFO
S28
DESIGNATED POSITION EXISTS ?
NO
DESIGNATION ERROR INFO
YES
S29
WRITE DATA
S30
DEVELOP TRANSACTION SERIAL NO.
S31
INCREMENT TRANSACTION SERIAL NO.
2

FIG. 6C

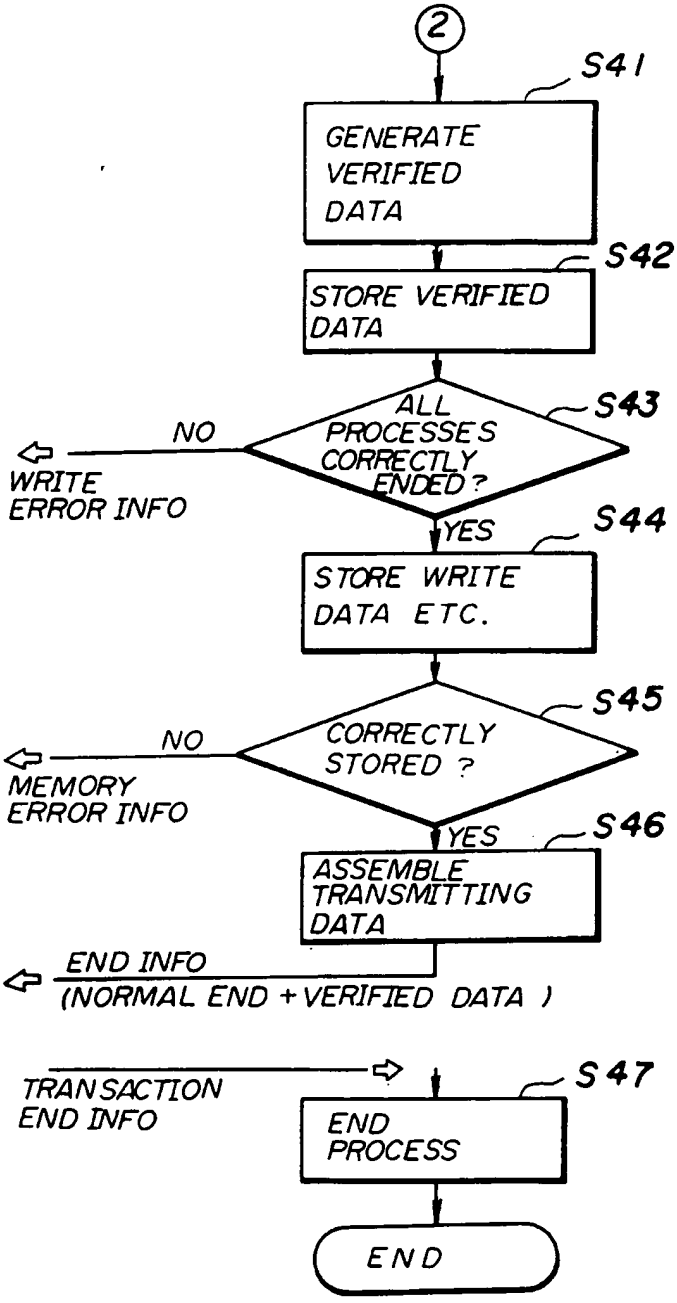
2
S41
GENERATE VERIFIED DATA
S42
STORE VERIFIED DATA
S43
ALL PROCESSES CORRECTLY ENDED ?
NO
WRITE ERROR INFO
YES
S44
STORE WRITE DATA ETC.
S45
CORRECTLY STORED ?
NO
MEMORY ERROR INFO
YES
S46
ASSEMBLE TRANSMITTING DATA
END INFO
(NORMAL END + VERIFIED DATA)
TRANSACTION END INFO
S47
END PROCESS
END

FIG. 7